ABSTRACT OF THE DISCLOSURE

According to each embodiment of the present invention, generation of key data different from each other can be guaranteed and the safety can be improved without providing a device for eliminating input of a specific pattern. Specifically, key data Kg2 to Kgm are generated by converting a common key K based on variables v_1 to v_{m-1} inputted independently from plain text blocks P1 to Pm or intermediate results i_1 to i_{m-1}. Therefore, in each embodiment of the present invention, even if the apparatus is attacked by a decryption technique by which the respective plain text blocks P1 to Pm are inputted as the same data, the key data Kg2 to Kgm can be created as values different from each other.